Cybersecurity Update

Gary Foster
April 10, 2017

massDOT
Massachusetts Department of Transportation

Discussion Topics

- **Cybersecurity Challenges**
- **Policy Work**
- **Security Awareness & Training**
- **Execution of Policies**
- **Next Steps**

Cybersecurity Challenges

38% ⬆
Increase in cybersecurity incidents in the past year.[1]

5 Months
Average time it takes to detect a security breach. [2]

48%
Percentage of data breaches that are caused by employees and contractors. [2]

A complex, moving target

Cyber threats are an increasing risk for MassDOT as professional hackers execute ever more sophisticated attacks against government agencies and private sector companies.

Commonwealth and MassDOT priority

The Commonwealth and MassDOT have identified cybersecurity as top priority. Cybersecurity is critical to MassDOT's ongoing ability to successfully perform its mission.

Cybersecurity begins with us

Cybersecurity is not simply an IT issue, it is an enterprise-wide responsibility. To successfully prevent, identify, and address cybersecurity threats, everyone's involvement is imperative.

[1] PwC Global State of Information Security Survey
[2] Ponemon Institute

massDOT Massachusetts Department of Transportation

Policy Work

16 **Information security policies created…**

189 **Internal controls developed…**

100% **Policies and internal controls have been signed off as draft by MassDOT senior leadership for implementation**

The first policy to be implemented is Security Awareness & Training.

Security Awareness & Training

The Security Awareness & Training program is being delivered in three phases. Phase 1, the current project, defines the program and establishes the approach for subsequent work.

Current Project
March – May

1. Leadership training and awareness campaign
2. Comprehensive training plan
3. Multi-channel communications strategy
4. Training content requirements

PHASE 1
Define Program

Summer – Fall 2017

PHASE 2
Launch Training

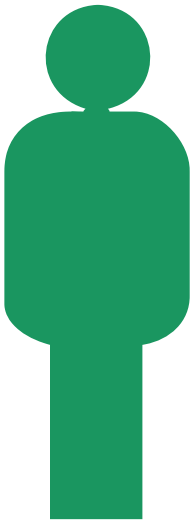
- Deliver online training according to plan
- Track and enforce compliance

PHASE 3
Maintain Program

- Measure outcomes
- Repeat training
- Track and enforce compliance

Execution of Policies

Based on a survey distributed to MassDOT information system users, respondents see cybersecurity as important, and are receptive to training and additional knowledge.



87.8%

See cybersecurity as important and necessary

8.6%

Cybersecurity is inconvenient but necessary

3.1%

Uncertain

0.5%

Cybersecurity is unimportant and unnecessary

Of the comments provided, 41% related to the need to change current practices; *passwords* were the most frequently cited pain point.

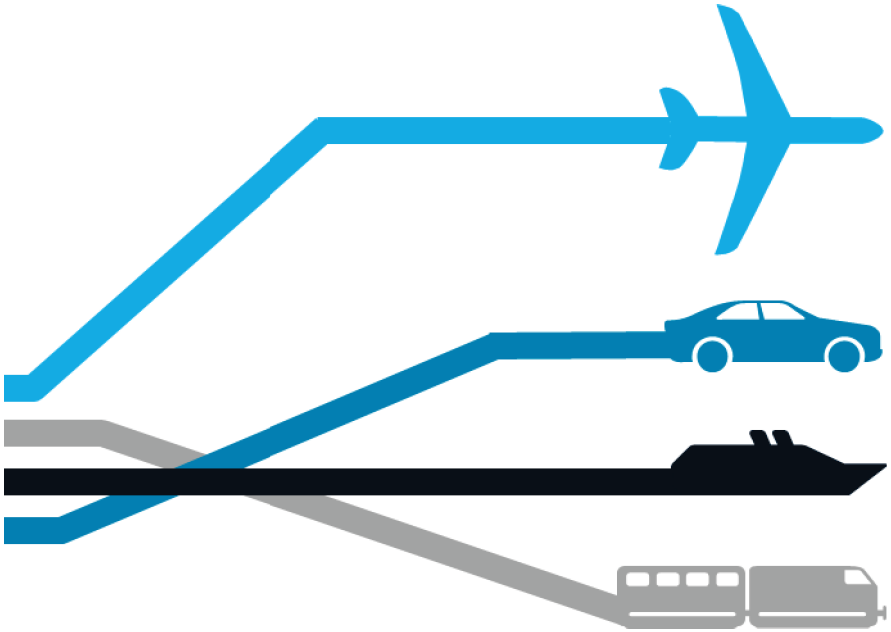
41%

39%

*Surface area of graphics are scaled to match percentage proportions

Next Steps

There are several components that are essential to the success of the Security Awareness & Training program.



Leadership support

Will be essential for communicating the value of the program and gaining buy-in

Receptive adoption

Change management is crucial to successfully implementing the training and adopting cybersecurity best practices

Enterprise-wide involvement

Cybersecurity needs to be the responsibility of every division, not only IT

Ongoing input

With your continued input, the implementation will have best chance at succeeding short-term and being sustainable long-term